NASA Procedural Requirements

NPR 1382.1A
Effective Date: July 10, 2013
Expiration Date: November 30, 2021

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

NASA Privacy Procedural Requirements

Responsible Office: Office of the Chief Information Officer

Table of Contents

Preface

P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 Applicable Documents and Forms
P.5 Measurement/Verification
P.6 Cancellation

Chapter 1. Privacy Management

1.1 Overview
1.2 Governing Statutes Overview

Chapter 2. Privacy Leadership

2.1 Privacy Roles and Responsibilities

Chapter 3. Privacy Risk Management and Compliance

3.1 Privacy Risk Management and Compliance Overview
3.2 Privacy Risk Management and Compliance Policy
3.2.1 Collecting Personally Identifiable Information
3.2.2 Privacy Impact Assessments
3.2.3 Privacy Act System of Records Notices
3.2.4 Privacy Act (e)(3) Statements
3.2.5 Computer Matching Agreements

Chapter 4. Privacy and Information Security

4.1 Privacy and Information Security Overview
4.2 Privacy and Information Security Policy

Chapter 5. Privacy Incident Response and Management

5.1 Privacy Incident Response and Management Overview
5.2 Privacy Incident Response and Management Policy

Chapter 6. Privacy Notice and Redress

6.1 Privacy Notice and Redress Overview
6.2 Privacy Notice and Redress Policy

6.2.1 Privacy Notice
6.2.2 Web Measurement and Customization Technology Use and Notice
6.2.3 COPPA Notice
6.2.4 Privacy Complaints
6.2.5 Privacy Redress and Privacy Act Information Requests

Chapter 7. Privacy Awareness and Training

7.1 Privacy Training and Awareness Overview
7.2 Privacy Training and Awareness Policy

Chapter 8. Privacy Accountability

8.1 Privacy Accountability Overview
8.2 Privacy Accountability Policy
8.2.1 Internal Reporting Requirements
8.2.2 External Reporting Requirements

Chapter 9. Privacy Rules of Behavior and Consequences

9.1 Privacy Rules of Behavior and Consequences Overview
9.2 Privacy Rules of Behavior and Consequences Policy
9.2.1 Privacy Rules of Behavior
9.2.2 Privacy Consequences

Appendix A. Definitions
Appendix B. Acronyms
Appendix C. Responsibilities Crosswalk
Appendix D. Role Definitions
Appendix E. References

Preface

P.1 Purpose

a. The purpose of this document is to set forth the procedural requirements for safeguarding individual privacy through the protection of personally identifiable information (PII), regardless of format, which is collected, used, maintained, and disseminated by the National Aeronautics and Space Administration (NASA).

b. This NASA Procedural Requirement (NPR) is based on Federal requirements as listed in section P.4, Applicable Documents and Forms. State requirements such as those issued under California law, which are more restrictive than NASA policy, should be followed, as applicable.

P.2 Applicability

a. This NPR is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers.

(1) For the purposes of this NPR, NASA Headquarters is regarded as a Center. All stated Center requirements are also applicable to NASA Headquarters.

b. This language applies to the Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center (FFRDC), other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

c. This NPR applies to PII collected, stored, used, processed, disclosed, or disseminated in any format for use by or on behalf of NASA and includes PII collections that are maintained externally through a contract or outsourced to: (1) a Government Owned, Contractor Operated (GOCO) facility; (2) partners under the Space Act; (3) partners under the Commercial Space Act of 1997; or (4) commercial or university facilities.

(1) External collections that are not gathered on behalf of NASA or are merely incidental to a contract (e.g., PII in a contractor's payroll and personnel management system) are excluded from this NPR and are considered non-NASA data.

(2) This NPR does not apply to PII collected and/or maintained by NASA employees and contractors for personal use (e.g., contact information for family, relatives, and doctors), as allowed under NASA Policy Directive (NPD) 2540.1, Personal Use of Government Office Equipment Including Information Technology.

d. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

P.3 Authority

a. National Aeronautics and Space Act, as amended, 51 United States Code (U.S.C.) § 20101 et seq.

b. E-Government (e-Gov) Act of 2002, as amended, 44 U.S.C. § 3601 et seq.

c. Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

d. NPD 1382.17, NASA Privacy Policy.

P.4 Applicable Documents and Forms

a. NASA Privacy Act Regulations, 14 Code of Federal Regulations (CFR) Part 1212.

b. The Federal Acquisition Regulations (FAR) Subpart 24.1 - Protection of Individual Privacy and the NASA FAR Supplement (NFS), Subpart 1824.1.

c. Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §6501, et seq., 16 C.F.R § 312.

d. Computer Matching and Privacy Protection Act of 1988, Public Laws (P.L.) 100-503.

e. Clinger-Cohen Act of 1996, 40 U.S.C. 11103.

f. Paperwork Reduction Act of 1995 (PRA), 44 U.S.C. § 3501, et seq.

g. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq.

h. Office of Management and Budget (OMB) M-05-08, Designation of Senior Agency Officials for Privacy

i. OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information.

j. OMB Memorandum M-06-16, Protection of Sensitive Agency Information.

k. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investment.

l. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

m. OMB Memorandum M-10-22, Guidance for Online use of Web Measurement and Customization Technologies, June 25, 2010.

n. OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications

o. OMB Circular A-130, Management of Federal Information Resources

p. NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology.

q. NPR 1441.1, NASA Records Retention Schedules.

r. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations.

s. NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

t. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

u. Information Technology Security Handbook (ITS-HBK)-1382.02, Privacy Goals and Objectives.

v. ITS-HBK-1382.03, Privacy Risk Management and Compliance.

w. ITS-HBK-1382.04, Privacy and Information Security.

x. ITS-HBK-1382.05, Privacy Incident Response and Management.

y. ITS-HBK-1382.06, Privacy Notice and Redress.

z. ITS-HBK-1382.07, Privacy Training and Awareness.

aa. ITS-HBK-1382.08, Privacy Accountability.

bb. ITS-HBK-1382.09, Privacy Rules of Behavior and Consequences.

cc. ITS-HBK-2810.03, Planning

dd. ITS-HBK-2810.06, Awareness and Training.

ee. ITS-HBK-2810.09, Incident Response and Management.

ff. ITS-HBK-2810.11, Media Protection.

P.5 Measurement/Verification

a. The obligation to measure performance is driven by Federal regulatory and NASA privacy requirements outlined within this NPR and the related handbooks. These measurements are based upon NASA's privacy goals and the objectives outlined by the Senior Agency Official for Privacy (SAOP), designed to provide substantive justification for decision making for the SAOP and senior management, which is utilized to measure the effectiveness of the NASA Privacy Program, its policies, and requirements.

b. The SAOP shall provide assessments and evaluations of the application of this NPR. This will consist of periodic reporting from the Centers, including information collected for the satisfaction of OMB and FISMA reporting requirements.

c. All covered entities are subject to privacy compliance reviews and evaluations by NASA.

P.6 Cancellation

a. NPR 1382.1, NASA Privacy Procedural Requirements, August 10, 2007.

b. NASA Information Technology Requirement (NITR)-1382-2, NASA Rules and Consequences Policy. Relative to Safeguarding Personally Identifiable Information (PII), January 28, 2008.

/S/
Larry N. Sweet
NASA Chief Information Officer

Chapter 1 - Privacy Management

1.1 Overview

1.1.1 This NPR establishes the privacy requirements and responsibilities for NASA, relative to the policy set forth in NPD 1382.17, NASA Privacy Policy. This document is intended to provide a framework for privacy program management and serves as the mechanism for the authorization of more in-depth documents (e.g., handbooks and memos).

1.1.2 This NPR is organized into eleven major sections: (1) Preface; (2) Management; (3) Leadership; (4) Risk Management and Compliance; (5) Information Security; (6) Incident Response and Management; (7) Notice and Redress; (8) Awareness and Training; (9) Accountability; (10) Rules of Behavior and Consequences; and (11) Appendices. Individual roles and responsibilities are included in sections 1-10, as appropriate. See Appendix C, Responsibilities Cross-Walk for a breakdown of applicable sections.

1.1.3 NASA is committed to protecting the privacy of information of individuals from whom it collects, maintains, uses, and/or disseminates such information.

1.1.3.1 Laws, regulations, and guidance documents provide various terms and definitions used to describe personal information. These include: personally identifiable information or PII, privacy information, Privacy Act records, and information in identifiable form (IIF).

(a) In this NPR, sensitive PII does not include official business contact information (e.g., work e-mail address, office location, and/or office telephone number) for NASA employees and contractors unless this information is assessed as sensitive PII due to use and context. Sensitive PII is a subset of PII, which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

1.1.4 The NASA SAOP establishes and maintains the Agency's privacy program and its overall objectives and priorities.

1.1.4.1 Privacy goals and objectives are identified and governed by ITS-HBK-1382.02, Privacy Goals and Objectives.

1.2 Governing Statutes Overview

1.2.1 This section provides a summary of each of the applicable governing statutes and their basic privacy-related requirements. The specifics of the related requirements and responsibilities are elaborated in subsequent chapters, as appropriate.

1.2.2 The Federal statutes that impact NASA's collection and management of PII include the Privacy Act, COPPA, e-Gov Act, FISMA, and the PRA.

1.2.2.1 Privacy Act of 1974 - The Privacy Act sets forth extensive requirements for the management of personal information contained in a system of records (SOR), where such information is routinely retrieved by a name or personal identifier unique to the individual.

1.2.2.2 Children's Online Privacy Protection Act of 1998 - COPPA regulates NASA's operation of

Web sites or online services directed to children under age 13 when the Web site or service collects personal information from children.

1.2.2.3 E-Government Act of 2002 - The e-Gov Act reinforces existing statutory privacy provisions and adds new requirements to ensure sufficient protections for the privacy of personal information as agencies implement electronic government.

(a) Title III of the e-Gov Act, or FISMA, provides for development and maintenance of minimum controls required to protect Federal information and information systems (including privacy information). The e-Gov Act also authorizes OMB and NIST to define "minimum controls required."

(b) Section 208 of the e-Gov Act requires NASA to complete Privacy Impact Assessments (PIAs) for new or modified information systems that collect, maintain, or disseminate IIF from or about members of the public.

1.2.2.4 Paperwork Reduction Act of 1995 - The PRA regulates the burden that agencies place on members of the public when collecting information from them. OMB authorization shall be obtained when NASA collects information from ten or more members of the public through standardized fields, whether via survey (in paper or electronic form), Web-enabled forms, or any method of information provisioning, regardless of format or whether the provisioning of the information is voluntary. For this NPR, the PRA is applicable only when NASA seeks collection of IIF from members of the public.

Chapter 2 - Privacy Leadership

2.1 Privacy Roles and Responsibilities

2.1.1 The following are overarching roles and responsibilities related to NASA's privacy program. Specific roles and responsibilities, as related to the elements of the privacy program, are referenced throughout the remainder of this NPR in their respective chapters.

2.1.1.1 NASA Headquarters, Centers, satellite and component facilities, and support service contractor sites may use internal organizational structure to fulfill the roles and responsibilities described herein, if the approach is documented in a formal policy.

2.1.2 Throughout this document, roles and responsibilities are generally listed at the highest level possible, with the assumption that specific tasks and functions may be delegated as necessary unless explicitly prohibited, (e.g., a conflict of interest or separation of duties is created).

2.1.2.1 The NASA Administrator shall:

a. Ensure the protection of PII within NASA's information and information systems.

b. Assign an SAOP.

c. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, NASA Records Retention Schedules, as appropriate.

2.1.2.2 The NASA Chief Information Officer (CIO) shall:

a. Provide guidance to the SAOP.

b. Issue NITRs to keep the NASA privacy program current with changes in federal privacy policy and guidelines, and with changes in the privacy environment, as needed.

c. Ensure that existing privacy NITRs are incorporated into future versions of this NPR and that once a NITR has been incorporated into the NPR, the NITR is canceled.

d. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.3 The SAOP shall:

a. Provide overall responsibility and accountability for ensuring NASA's implementation of privacy information protections.

b. Ensure that NASA is compliant with applicable Federal laws, regulations, policies, guidelines, and NASA privacy program requirements.

c. Develop and maintain a NASA-wide privacy program.

d. Develop NASA privacy goals and objectives.

e. Approve handbooks related to this NPR.

f. Assign a Privacy Program Manager to oversee the NASA-wide privacy program.

g. Assign a NASA Privacy Act Officer responsible for oversight of NASA's compliance with the Privacy Act.

h. Advise senior NASA officials concerning their responsibilities to protect privacy information.

i. Evaluate legislative, regulatory, and other guidelines and policies related to privacy.

j. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.4 The Center/Executive Director shall:

a. Appoint a Center Privacy Manager (CPM).

b. Support the protection and management of PII at the Center and consult with the CPM on matters pertaining to privacy.

c. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.5 The Center CIO shall:

a. Ensure that all Center information and information systems comply with the provisions of this NPR.

b. Support the protection and management of PII at the Center and consult with the CPM on matters pertaining to privacy. Support the CPM in protecting PII and/or IIF at the Center.

c. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.6 The Senior Agency Information Security Officer (SAISO) shall:

a. Provide necessary management and resources in support of the NASA-wide privacy program as established by the SAOP.

b. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.7 The NASA Privacy Program Manager shall:

a. Oversee and manage the development and implementation of policy and procedure, guidance, directives, and requirements for NASA in support of compliance with Federal laws, statutes, and Government-wide policy as directed by the SAOP.

b. Ensure that NASA complies with privacy requirements within Federal statutes, including the collection, maintenance, use, and dissemination of privacy information.

c. Develop and maintain NASA privacy policies, procedural requirements, and handbooks as directed by the SAOP.

d. Oversee and provide guidance in the implementation and the day-to-day operation of the NASA-wide privacy program as directed by the SAOP.

e. Review NASA's compliance with information privacy laws, regulations, and policies annually to validate effectiveness and ensure conformity with current Federal policies and guidance as directed by the SAOP.

f. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.8 The NASA Privacy Act Officer shall:

a. Ensure compliance with requirements of the Privacy Act.

b. Oversee, manage, and implement the Privacy Act requirements for NASA.

c. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.9 The Center Chief Information Security Officer (CISO) shall:

a. Support the CPM in protecting PII at the Center.

b. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.10 The CPM shall:

a. Serve as the Center advisor to the Center Director, Center CIO, Center CISO, and Information System Owners (ISOs) on all matters pertaining to privacy.

b. Function as the primary Center point of contact/liaison to the NASA Privacy Program Manager and NASA Privacy Act Officer.

c. Work with ISOs to review and aid in ensuring compliance with all privacy requirements, as needed.

d. Validate the proper disposition and/or sanitization process for files and records (paper, electronic, or other media formats), which contain privacy information.

e. Ensure the NASA privacy program is implemented at the Center in accordance with NASA policy.

f. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.11 The ISO shall:

a. Acquire, develop, integrate, operate, modify, maintain, and dispose of information systems containing PII in a manner consistent with Federal statutes, regulation, and NASA privacy policies.

b. Ensure compliance with Privacy Act for applications and information systems containing Privacy Act records.

c. Verify with the Contracting Officer (CO)/Contracting Officer Technical Representative (COTR) that any contract that requires the operation of an SOR on behalf of NASA includes the appropriate FAR clauses required per FAR Subpart 24.1—Protection of Individual Privacy.

d. Notify the CO when purchase requests include services covered by the Privacy Act or PRA.

e. Notify the CO when contractor services will require or include access to PII collected by or on behalf of NASA.

f. Ensure that the contract statement of work identifies this NPR as outlining the NASA-specific requirements that must be followed by the contractor.

g. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

2.1.2.12 The NASA User shall: a. Comply with all Federal laws, statutes, Government-wide, and NASA privacy policies and procedures.

b. Protect all PII in their custody, virtual, electronic, actual, or otherwise from unauthorized disclosure, use, modification, or destruction so that the confidentiality and integrity of the information are preserved.

c. Manage and dispose of records created as a result of the requirements of this NPR in accordance with NPR 1441.1, as appropriate.

Chapter 3 - Privacy Risk Management and Compliance

3.1 Privacy Risk Management and Compliance Overview

3.1.1 The Privacy Risk Management and Compliance chapter ensures NASA's compliance with requirements for the collection, assessment, and notice of PII. Additional information on privacy notice is located in Chapter 6, Privacy Notice and Redress.

3.1.2 NASA is responsible for assessing the PII it collects and notifying individuals of what information is collected, why it is being collected, and how the information will be used. In accordance with the Privacy Act, e-Gov Act, and OMB requirements, NASA uses compliance documentation such as PIAs, and Privacy Act System of Records Notices (SORNs). These tools assist NASA in identifying and reducing the privacy risks related to NASA's activities, notifying the public of privacy impacts, and determining which steps to take to mitigate potential impacts to personal privacy. All NASA applications, information systems, and Web sites shall be reviewed via the Initial Privacy Threshold Analysis (IPTA) process to determine whether or not they require a complete PIA.

3.1.3 NASA Privacy Risk Management and Compliance procedures are governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2 Privacy Risk Management and Compliance Policy

3.2.1 Collecting Personally Identifiable Information

The collection of PII during the course of official government business is permitted as long as: (1) authorized by law, (2) Federal and NASA privacy requirements are satisfied, and (3) is otherwise necessary to a NASA program and/or its associated mission. Specific information on collecting PII is governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.1.1 The SAOP shall:

a. Limit the collection of PII to that which is legally authorized, consistent with Federal and NASA privacy requirements, and to the minimum extent necessary.

b. Ensure that PII is collected only when necessary for the proper performance of NASA's functions and mission support.

c. Conduct annual review activities to reduce or eliminate unnecessary collections of PII.

3.2.1.2 The NASA Privacy Program Manager shall coordinate and direct annual NASA-wide review activities to reduce or eliminate unnecessary collections of PII.

3.2.1.3 The CPM shall:

a. Work with ISOs to ensure that all PII is maintained with accuracy, relevance, timeliness, and completeness.

b. Coordinate annual review activities at the Center level with ISOs to ensure PII is collected in accordance with this policy and to reduce or eliminate unnecessary collections of PII.

c. Work with ISOs to eliminate the unnecessary use of social security numbers (SSNs).

3.2.1.4 The ISO shall:

a. Eliminate the collection of information if the information is not necessary to a NASA program and/or its associated mission.

b. Ensure that all privacy information is maintained with accuracy, relevance, timeliness, and completeness.

c. Ensure that Privacy Act records are collected and maintained in accordance with NASA Privacy Act policies.

d. Conduct annual review activities to reduce or eliminate unnecessary collections of PII.

e. Avoid the collection of SSNs, in accordance with NPD 1382.17, unless required by statute or some another requirement mandating the use of SSNs.

3.2.2 Privacy Impact Assessments

a. A PIA is a formal process through which NASA analyzes how information is processed by an information system, application, or Web site to ensure that its handling conforms to applicable statutory, regulatory, and policy requirements for privacy information. IIF is information that identifies an individual, directly or indirectly. The PIA is used to determine the risks and effects of collecting, maintaining, and disseminating IIF on members of the public. NASA conducts PIAs under two circumstances: (1) in accordance with Section 208 of the e-Gov Act and NIST SP 800-53, for any new or substantially changed information system that collects, maintains, or disseminates IIF from or about members of the public (under the e-Gov Act, members of the public exclude Government personnel, contractors, and partners); or (2) for a new collection of ten or more members of the public in accordance with the PRA.

b. NASA has developed an assessment process to evaluate the nature of the information to be collected and maintained. Responses in the IPTA lead to the determination of what actions shall be taken to comply with applicable statutes, including whether completion of a PIA is required.

c. A PIA describes the information to be collected; the purpose of the collection (why it is collected and its intended use); with whom the information will be shared; if the information was collected with the consent of the owner - or the owner's parent or guardian, if needed (in accordance with COPPA); how the information will be secured; and whether a SOR is created under the Privacy Act. In addition, the PIA examines and documents the evaluation of protections and alternative processes for handling information to mitigate potential privacy risks. Unless otherwise prohibited, NASA is responsible for posting the PIA publicly.

d. Information Security Controls, NIST SP 800-53 PL-5 is governed at NASA by ITS-HBK-2810.03, Planning and ITS-HBK-1382.03, Risk Management and Compliance.

e. Specific information on how to conduct an IPTA and a PIA: review, approval, publication requirements, and the relationship to the PRA and the Privacy Act are governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.2.1 The SAOP shall:

a. Establish Agency policy, requirements, and process for conducting IPTAs and/or PIAs for new or revised applications and information systems.

b. Assess the impact of technology on privacy and the protection of personal information.

c. Approve all completed PIAs.

3.2.2.2 The Center CIO shall ensure that an IPTA, and as appropriate a PIA, is conducted for every application and information system, including Web sites.

3.2.2.3 The NASA Privacy Program Manager shall:

a. Develop and implement Agency policy, requirements, and processes for conducting IPTAs and PIAs as appropriate, for new or revised applications and information systems.

b. Ensure PIAs are thorough and meet all applicable standards.

c. Ensure that completed PIAs are made publicly available for applications and information systems, including Web sites, which collect and/or maintain IIF on members of the public, consistent with Federal policy.

3.2.2.4 The CPM shall:

a. Assist ISOs in the completion of IPTAs and, as appropriate, PIAs.

b. Conduct timely reviews of applications and information systems, including Web sites, IPTAs and PIAs to ensure the ISO has addressed adequate protection of privacy and/or Privacy Act information.

c. Ensure the ISOs update IPTAs and, as appropriate, PIAs.

d. Conduct annual PIA reviews.

3.2.2.5 The ISO shall:

a. Ensure that an IPTA is conducted and approved for the applications and information systems, including Web sites, under their purview.

b. Ensure that a PIA is reviewed and approved, as appropriate for:

(1) An information system that collects, maintains, or disseminates IIF from or about members of the public; or

(2) An electronic collection of IIF for ten or more individuals, consistent with the PRA.

c. Ensure that all applications and information systems, including Web sites, following significant modification, conduct a re-evaluation of IPTAs and, as appropriate, PIAs.

d. Ensure that a PIA is conducted prior to use of a third-party Web site or application.

e. Review completed PIAs annually to ensure ongoing accuracy.

3.2.3 Privacy Act System of Records Notices

In accordance with the Privacy Act, a SORN is required for each NASA SOR containing

information on individuals from which records are retrieved by an individual identifier (i.e., name of the individual or by some unique number, symbol, or other identifier assigned to an individual). In order to meet statutory requirements, a SORN shall be published in the Federal Register prior to any collection or new use of information in a Privacy Act system. Specific information on the review, approval, and publication requirements for a SORN are governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.3.1 The SAOP shall:

a. Provide guidance on the development and publication of SORNs.

b. Review and issue all SORNs for publication in the Federal Register.

3.2.3.2 The NASA Privacy Act Officer shall:

a. Review and revise draft SORNs.

b. Coordinate the Agency review and the SAOP signature of the SORN for submission to the Federal Register for publication through the NASA Federal Register Liaison Officer.

c. Coordinate with CPMs in determining whether an existing NASA or other government SORN covers Privacy Act records maintained by NASA.

3.2.3.3 The CPM shall:

a. Work with ISOs in identifying the need for a Privacy Act SORN.

b. Assist the ISO in drafting a SORN for publication in the Federal Register, if not already covered under an existing SORN.

c. Provide the NASA Privacy Act Officer with draft SORNs, as required.

d. Conduct SORN reviews, as required.

e. Coordinate the review and approval of new draft SORNs and Privacy Act notice updates with ISOs and the NASA Privacy Act Officer.

3.2.3.4 The ISO shall:

a. Limit the maintenance of Privacy Act records on individuals that are retrievable by name or other personal identifier to only those instances for which a Privacy Act SORN has been published in the Federal Register.

b. Draft a SORN for publication in the Federal Register, if not already covered under an existing SORN.

c. Work with the CPM and the NASA Privacy Act Officer to publish a SORN in the Federal Register.

3.2.4 Privacy Act (e)(3) Statements.

In accordance with the Privacy Act, individuals who are asked to provide information that will be maintained in a NASA Privacy Act SOR are required at the point of collection to be presented with a Privacy Act 5 U.S.C. § 552(a)(e)(3) Statement (hereinafter referred to as a Privacy Act Statement). The Privacy Act Statement requirement may be accomplished through a standalone paper based

statement, a statement on the paper or electronic form, or an electronic statement on a dedicated Web page. Specific information on Privacy Act Statement requirements is governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.4.1 The SAOP shall provide guidance on the use of Privacy Act Statements.

3.2.4.2 The NASA Privacy Act Officer shall work with the CPM to ensure the Privacy Act Statement meets the requirements of the Privacy Act.

3.2.4.3 The CPM shall work with ISOs to ensure the Privacy Act Statement meets the requirements of the Privacy Act.

3.2.4.4 The ISO shall:

a. Ensure that individuals who are asked to provide information to be maintained in a Privacy Act SOR are presented at the point of collection with a Privacy Act Statement that:

(1) Is presented either on the information collection sheet or screen, or via a separate sheet or screen that the individuals can print and retain;

(2) Complies with the requirements outlined in 14 CFR 1212.602; and

(3) Is in a format that the individual may be able to retain in a physical or hard copy.

b. Ensure that new NASA forms or Center forms created for the collection of SOR information provide the correct and specific Privacy Act Statement for that SOR.

3.2.5 Computer Matching Agreements.

In accordance with the Privacy Act, as amended by the Computer Matching and Privacy Protection Act of 1988, a public notice of the proposed match and the computer matching agreement is required to be published in the Federal Register before NASA can match its data with another Federal entity or state government. Specific information on Computer Matching Agreement requirements governed by is detailed in ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.5.1 The NASA SAOP shall:

a. Establish a Data Integrity Board that is responsible for approving, overseeing, and coordinating the matching program before any ISO may engage in a computer matching program as defined by the Privacy Act.

b. Provide guidance on computer matching agreements.

3.2.5.2 The NASA Privacy Act Officer shall work with the ISO to prepare and publish a notice in the Federal Register at least 30 days in advance of the establishment or revision of a matching program.

3.2.5.3 The ISO shall prepare and publish a notice in the Federal Register at least 30 days in advance of the establishment or revision of a matching program, in coordination with the NASA Privacy Act Officer.

Chapter 4 - Privacy and Information Security

4.1 Privacy and Information Security Overview

4.1.1 The Privacy and Information Security chapter relates to NASA's initiatives for privacy and information security. This chapter addresses requirements that all NASA PII shall be secured, as directed by the Privacy Act; e-Gov Act; OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information; OMB Memorandum M-06-16, Protection of Sensitive Agency Information; OMB Memorandum M-06-19, Reporting Incidents Involving PII and Incorporating the Cost for Security in Agency Information Technology Investment; OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information; and NIST SP 800-122, Guide for Protecting the Confidentiality of Personally Identifiable Information (PII).

4.1.2 NASA has a responsibility to protect the confidentiality, integrity, and availability of NASA information and information systems. The categorization of information systems may be Low, Moderate, or High as defined in NIST SP 800-60 and Federal Information Processing Standards (FIPS). Information systems containing PII are categorized at a minimum Confidentiality level of Moderate. Information systems with non-sensitive PII may be categorized at a Confidentiality level of Low, as permitted by the information types.

4.1.3 All PII shall be handled and protected as sensitive information (i.e., SBU/CUI) in accordance with current NASA Security Program Procedural Requirements for sensitive information.

4.1.4 NASA Privacy and Information Security procedures are governed by ITS-HBK-1382.04, Privacy and Information Security.

4.2 Privacy and Information Security Policy

4.2.1 The SAOP shall implement privacy policies and procedures to ensure the confidentiality and integrity of privacy information.

4.2.2 The Center CISO, jointly with the CPM, shall ensure that the protection of privacy information is maintained throughout the creation, transmission, storage, use, and disposition of information.

4.2.3 The CPM, jointly with the Center CISO, shall ensure that the protection of privacy information is maintained throughout the creation, transmittal, storage, use, and disposition of information.

4.2.4 The ISO and User supervisors shall:

a. Ensure that access to PII is limited to those NASA users who have a need for access.

b. Ensure the protection of PII from unauthorized access or disclosure throughout its life cycle.

c. Ensure the information types used within the security plan, and which contain PII, are categorized at a minimum Confidentiality level of Moderate during the FIPS assessment. This does not affect information types that only include non-sensitive PII.

d. Ensure development and documentation of administrative, technical, and physical safeguards that

protect against any anticipated threats or hazards to the security or integrity of records and against the potential of their unauthorized use in accordance with the requirements outlined in NPR 2810.

e. Ensure all computer-readable data extracts from databases containing PII are logged and verified to the extent possible, including information on whether the extracted data have been erased within 90 days or that the data's use is still required.

f. Ensure PII is encrypted on any mobile medium (e.g., e-mail, memory stick, CD/DVD, etc.), at rest, and that other security controls are in place to render PII unusable by unauthorized individuals.

4.2.5 The NASA User shall:

a. Limit disclosure of information on individuals from a SOR as provided only in accordance with 14 CFR 1212 routine uses of the Privacy Act records published in the applicable SORN.

b. Request Privacy Act records only under appropriate authority.

c. Ensure that any PII on mobile devices is safeguarded, at a minimum, using encryption solutions which are compliant with Federal encryption algorithm standards and NIST guidance, and in accordance with current NASA Security Program Procedural Requirements for sensitive information.

d. Ensure that PII is protected during transmission, at a minimum, using encryption solutions which are compliant with Federal encryption algorithm standards, NIST guidance, and in accordance with current NASA Security Program Procedural Requirements for sensitive information.

e. Ensure that all PII transmitted or downloaded, in any format or media, to or from mobile devices is properly encrypted according to NASA Security Program Procedural Requirements for sensitive information.

f. Label any mobile device or portable media containing PII in accordance with current NASA Security Program Procedural Requirements for sensitive information.

g. Remove PII from Agency premises or download and store PII remotely only under conditions prescribed in current NPRs for sensitive information.

h. Ensure the proper disposition and/or sanitization of files, records, and/or media containing privacy information in accordance with the standards outlined in ITS-HBK-2810.11, Media Protection.

Chapter 5 - Privacy Incident Response and Management

5.1 Privacy Incident Response and Management Overview

5.1.1 The Privacy Incident Response and Management chapter relates to NASA's response to incidents involving the breach of PII entrusted to NASA's custody or managed by a contractor on NASA's behalf. This chapter addresses breach response requirements within OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investment, and OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

5.1.2 The mechanism for response to a confirmed moderate or high-risk breach is a privacy Breach Response Team (BRT), which is convened within 24 hours of the incident. A Center BRT is convened when a breach of sensitive PII meets the threshold outlined in the handbooks associated with Chapter 5. Sensitive PII is a subset of PII, which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. The BRT analyzes risk of identity theft in accordance with OMB requirements and NASA policies and guidelines, prepares recommendations for remediation and notification plans, drafts breach notification letters, determines the mechanism of public notice, assists the ISO in preparing Frequently Asked Questions (FAQs), notifies and continues to provide updates to the NASA Privacy Program Manager on the status of the breach and any related breach response activities, and submits findings and recommendations to the SAOP for approval, as appropriate.

5.1.3 Non-governmental PII that is the property of the custodian, or entrusted to that person by friends or family, or a NASA contractor, grantee, etc., including corporate data used for non-governmental purposes but stored on NASA equipment is not covered by this NPR. While the limited personal use of government equipment may be permitted by NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology, NASA has no responsibility for the loss or compromise of such information.

5.1.4 NASA privacy breach response procedures are governed by ITS-HBK-1382.05, Privacy Incident Response and Management and ITS-HBK-2810.09, Incident Response and Management.

5.2 Privacy Incident Response and Management Policy

5.2.1 The SAOP shall:

a. Establish, implement, and publish Agency PII breach response and management policies and procedures in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

b. Review, approve, or amend BRT recommended actions and notification plans, as appropriate.

c. Advise NASA senior management on sensitive PII breaches and remediation progress, as appropriate.

d. Activate an Agency BRT if the situation warrants a NASA-wide activation.

e. Advise NASA senior management when notification and action plans need to be executed at a NASA-wide level.

f. Ensure that all NASA users receive incident reporting training as outlined in Chapter 7 of this NPR.

5.2.2 The Center CIO shall advise the BRT, as appropriate.

5.2.3 The NASA Privacy Program Manager shall:

a. Assist the SAOP in fulfilling PII breach responsibilities.

b. Recommend to the SAOP to activate an Agency BRT, if appropriate, and not already activated.

c. Maintain, as appropriate, coordination and communication with the SAISO and the NASA Security Operations Center (SOC) for incident reporting, tracking, and closure of sensitive PII breaches.

d. Provide, as necessary, overall direction to an Agency BRT for sensitive PII breaches.

e. Provide overall breach response guidance for sensitive PII BRT activities.

f. Update the SAOP on the status of the breach and breach response activities, as appropriate.

g. Submit, as appropriate, BRT findings and recommendations to the NASA SAOP for approval.

5.2.4 The CPM shall:

a. Ensure suspected loss, actual loss, and unauthorized access to PII are reported in accordance with NASA policy and procedures.

b. Function as a core Center BRT member advising the BRT on privacy related policy, requirements, and procedures.

c. Ensure that the steps outlined in ITS-HBK-1382.05 and ITS-HBK-2810.09 are met, as appropriate.

d. Participate in suspected PII breach initial investigations, determinations, reporting, and response efforts.

e. Produce reports and close out breach actions, as required.

f. Ensure necessary followup actions on remediation efforts, in coordination with the Center CISO, are conducted to reduce risk of repeat offenses.

5.2.5 The ISO shall:

a. Advise the BRT on the specifics of the affected information system(s) and/or information.

b. Advise on applicable policies, processes, and impacts related to the breach.

c. Support recommendations from the BRT.

5.2.6 The NASA user shall report any suspected or confirmed breach of any form of PII as an Information Security incident to the NASA SOC immediately upon discovery.

5.2.7 The Office of the Inspector General (OIG) shall investigate PII breaches involving suspected criminal intent in accordance with the OIG policies and coordinate with the BRT on such matters, as appropriate.

5.2.8 The Office of the General Counsel shall advise all BRTs on legal issues and review for legal sufficiency all proposed notification materials.

5.2.9 The Center Chief Counsel shall advise the Center BRT on legal issues and review for legal sufficiency proposed notification materials, as appropriate.

5.2.10 The Center Public Affairs Office may:

a. Advise on, and review, proposed notification materials and approaches.

b. Generate releases and other public notifications as requested.

5.2.11 The CO/COTR, in situations where the breach involves information maintained on NASA's behalf by or on contractors, shall serve as the interface between government and contracting parties.
5.2.12 The Center Human Resources Employee Relations Specialist may:

a. Designate an Human Resources staff member to serve as a member of the BRT. The designated staff member will participate in gathering and documenting information and evidence about the role of any civil servant employee in the breach.

b. Advise the civil servant's supervisor(s) on appropriate corrective action, which may include formal or informal disciplinary action.

Chapter 6 - Privacy Notice and Redress

6.1 Privacy Notice and Redress Overview

6.1.1 The Privacy Notice and Redress chapter relates to NASA's initiatives to ensure notice has been provided to the public and that a mechanism (i.e., policies and procedures) is in place to allow an individual to request information NASA has collected about them and, if needed, to redress or correct their information.

6.1.2 NASA Privacy Notice and Redress procedures are governed by 14 CFR 1212 and governed by ITS-HBK-1382.06, Privacy Notice and Redress.

6.2 Privacy Notice and Redress Policy

6.2.1 Privacy Notice

NASA provides general notice to the public in a number of ways, including the publishing of PIAs, SORNs, Privacy Act Statements, and the NASA Web Privacy Policy and Important Notices ("NASA Web Privacy Policy"). PIAs, SORNS, and Privacy Act Statements are addressed in Chapter 3. All publicly facing NASA Web sites shall link to the NASA Web Privacy Policy. This includes Web sites that are operated under contract that are deemed to be maintained by the Agency and all Web sites operated on behalf of the Agency. Posting the NASA Web Privacy Policy is not required if: 1) a Web site contains no "Government information," as defined in OMB Circular A-130 (i.e., information created, collected, processed, disseminated, or disposed of by or for the Federal Government); 2) a Web site is an Agency intranet Web site accessible only by authorized NASA users (employees, contractors, consultants, fellows, and grantees); or 3) a Web site is a National Security system, as defined in 40 U.S.C. 11103, or as exempt from the definition of information technology, as defined in Section 202(i) of the e-Gov Act. In accordance with OMB Memorandum M-10-23, the NASA Web Privacy policy is required to be included on official NASA Web sites and applications hosted on third-party Web sites and applications. Specific information on privacy notice requirements is governed by ITS-HBK-1382.06, Privacy Notice and Redress.

6.2.1.1 The NASA CIO shall:

a. Ensure the NASA Web Privacy Policy is posted (or linked to) all public facing NASA Web sites.

b. Ensure the NASA Web Privacy Policy is posted (or linked to) on official NASA Web sites and applications hosted on third-party Web sites and applications.

c. Make the NASA Web Privacy Policy available through the NASA Office of the CIO (OCIO) Web site.

d. Ensure that the NASA Web Privacy Policy is translated into a standardized machine-readable format.

6.2.1.2 The SAOP shall:

a. Ensure the NASA Web Privacy Policy:

(1) Includes description of the information being collected.

(2) Includes the purpose for the collection.

(3) Includes the official use of, or need for, the collected information.

(4) Specifies what information NASA collects automatically (e.g., user's internet protocol (IP) address, location and time of visit) and identifies the use for which it is collected (e.g., site management or security purposes).

(5) Informs visitors as to whether their provision of the requested information is voluntary.

(6) Informs visitors on how to grant consent for the use of voluntarily provided information.

(7) Informs visitors on how to grant consent for NASA to utilize the information that the Web site collects for a use other than statutorily mandated or authorized routine uses under the Privacy Act.

(8) Notifies visitors of their rights under the Privacy Act for SOR.

(9) Incorporates information to meet the requirements of the COPPA, where appropriate.

(10) Includes information on the redress mechanism.

(11) Notifies visitors as to how the Agency handles unsolicited e-mail, including the fact that the sender's privacy is not guaranteed.

b. Disclose, in the applicable NASA Web Privacy Policy, a third party's involvement in Agency applications when they are embedded within a NASA Web site.

6.2.1.3 The Center CIO shall:

a. Examine and monitor the third party's privacy policy when the Center uses a third-party Web site or application to evaluate risk and determine whether its use is appropriate for NASA.

b. Ensure the NASA Web Privacy Policy is incorporated into all Center public-facing NASA Web sites.

6.2.1.4 The Privacy Program Manager shall review the NASA Web Privacy Policy to ensure compliance with this NPR and Federal requirements, and recommend updates, as appropriate.

6.2.1.5 The CPM shall assist the Center CIO in ensuring the NASA Web Privacy Policy is incorporated into all Center public facing NASA Web sites.

6.2.1.6 The ISO shall:

a. Ensure that privacy policies clearly and concisely inform visitors of the collection of PII.

b. Ensure that Privacy Act notification is provided to anyone entering an information system containing Privacy Act records.

c. Incorporate the NASA Web Privacy Policy into public-facing NASA Web sites.

6.2.2 Web Measurement and Customization Technology Use and Notice.

Web measurement and customization technologies are used "... to remember a user's online interactions with a Web site or online application in order to conduct measurement and analysis of

usage or to customize the user's experience" per OMB Memorandum M-10-22. The use of this technology is permitted to improve NASA's online services; however, the use and notice requirements as outlined by OMB and NASA requirements shall first be satisfied. Specific information on when and how these technologies may be used at NASA is governed by ITS-HBK-1382.06, Privacy Notice and Redress.

6.2.2.1 The SAOP shall:

a. Ensure the NASA Privacy Policy describes the use of third-party Web sites and applications, as outlined by OMB.

b. Approve waivers for Web measurement and customization technology that collects PII prior to use of that technology, as defined in ITS-HBK-1382.06, and annually thereafter.

6.2.2.2 The Center CIO shall approve any Web measurement and customization technology use that does not collect PII prior to use of that technology, as defined in ITS-HBK-1382.06, and annually thereafter.

6.2.2.3 The NASA Privacy Program Manager shall advise the SAOP on Web Measurement and Customization Technology use at NASA.

6.2.2.4 The CPM shall advise the ISO on Web Measurement and Customization Technology use and requirements.

6.2.2.5 The ISO shall:

a. Ensure Web Measurement and Customization Technology use is compliant with requirements outlined in ITS-HBK-1382.06.

b. Ensure that the Web site utilizing approved Web Measurement and Customization Technology provides clear and conspicuous notice concerning the use of the technology and includes:

(1) The nature of the information collected.

(2) The purpose and use of the information.

(3) Whether, and to whom, the information will be disclosed.

(4) What privacy safeguards are applied to the information collected.

(5) Consequences to the visitor, or NASA user, of opting out.

c. Seek a waiver from the SAOP to use Web Measurement and Customization Technology when required, as described in ITS-HBK-1382.06.

6.2.3 COPPA Notice.

NASA Web sites that target children and collect PII from children under age 13 are required to provide conspicuous notice of the information collection practices, verifiable parental consent, and access, as defined by COPPA. Specific information on COPPA Notice requirements is governed by ITS-HBK-1382.06, Privacy Notice and Redress.

6.2.3.1 The Privacy Program Manager shall maintain Agency guidance for compliance with COPPA.

6.2.3.2 The ISO shall:

a. Ensure compliance with COPPA for Web sites intended to be used by, or targeted to, children under the age of 13 that collect PII.

b. Ensure that notice is provided concerning what information is being collected from children by the operator, how the information will be used, and the operator's disclosure practices.

c. Ensure verifiable parental approval is obtained for the collection, use, or disclosure of information from children.

d. Provide a process for parental review of information collected from the child.

e. Provide an opportunity for parental refusal to permit the operator's future use of the information or future collection of information.

f. Provide a means for the parent to obtain the personal information collected from the child.

6.2.4 Privacy Complaints

NASA is required to provide a mechanism for receiving and managing complaints from the public and from NASA users. Specific information on the privacy complaints process is governed by ITS-HBK-1382.06, Privacy Notice and Redress.

6.2.4.1 The SAOP shall:

a. Develop policies and procedures for managing privacy complaints and inquiries.

b. Establish a complaint process, which includes the mechanism for filing a complaint.

c. Ensure that complaints are recorded, tracked, and addressed.

6.2.4.2 The NASA Privacy Program Manager shall work with the SAOP to record, track, and address privacy complaints.

6.2.4.3 The CPM shall:

a. Receive and address Center-level privacy complaints, as appropriate.

b. Report Center-level privacy complaints to the NASA Privacy Program Manager via the process defined in ITS-HBK-1382.06.

6.2.4.4 The ISO shall:

a. Receive and address privacy complaints associated with the application, information system, or Web site, if appropriate.

b. Report application, information system, or Web site privacy complaints to the CPM.

6.2.5 Privacy Redress and Privacy Act Information Requests.

NASA shall provide a mechanism for redress and remedy from misuse or mishandling of PII and for correcting inaccuracies. Specifically, NASA shall provide the public and the NASA user with the opportunity to amend or correct their PII. Specific information on the redress process is governed by ITS-HBK-1382.06, Privacy Notice and Redress. Additionally, NASA shall respond to Privacy Act information requests in accordance with 14 C.F.R. 1212.

6.2.5.1 The SAOP shall:

a. Develop policies and procedures for redressing misuse or mishandling of PII and for correcting inaccuracies. These policies shall:

(1) Be in plain language and easy to read and understand.

(2) Explain the right of redress.

(3) Explain the process for complaining, seeking redress, and/or appealing adverse decisions.

(4) Provide a general timeline for the redress process.

(5) Identify the privacy policy related to PII being collected, processed, or maintained.

b. Permit individual access to the Privacy Act SOR in order to amend those Privacy Act records, as permitted in accordance with 14 C.F.R 1212.

6.2.5.2 The NASA Privacy Program Manager shall assist the SAOP in redressing PII issues.

6.2.5.3 The Privacy Act Officer shall process Privacy Act record access requests from an individual seeking access to their individual NASA maintained record in accordance with 14 C.F.R 1212 and the Privacy Act.

6.2.5.4 The CPM shall ensure Privacy Act record access requests are forwarded to the appropriate System Manager for processing in accordance with 14 C.F.R. 1212.

6.2.5.5 The System Manager shall process Privacy Act record access requests from an individual seeking access to their individual NASA maintained record in accordance with 14 C.F.R 1212 and the Privacy Act.

6.2.5.6 The Freedom of Information Act (FOIA) Officer shall process Privacy Act record access requests from an individual seeking access to their individual NASA maintained record in accordance with 14 C.F.R 1212 and the Privacy Act.

Chapter 7 - Privacy Awareness and Training

7.1 Privacy Awareness and Training Overview

7.1.1 The Privacy Awareness and Training chapter relates to NASA's initiatives to ensure that all NASA Users are aware of and trained on their roles and responsibilities related to PII. Several OMB documents outline the privacy training requirements, including OMB Circular A-130, OMB Memorandum M-05-08, and OMB Memorandum M-07-16. Specifically, OMB Memorandum M-07-16 provides that every NASA user is responsible for receiving training prior to gaining access to NASA information and information systems, with an annual requirement for refresher training thereafter. Additionally, advanced training may be required depending on the privacy-related responsibilities of the NASA user.

7.1.2 NASA Privacy Training and Awareness procedures are governed by ITS-HBK-1382.07, Privacy Awareness and Training, and ITS-HBK-2810.06, Security Awareness and Training.

7.2 Privacy Training and Awareness Policy

7.2.1 The SAOP shall:

a. Ensure NASA users receive appropriate training and education on their privacy responsibilities, including acceptable rules of behavior, when and how to report privacy related incidents, and consequences for violating this NPR.

b. Oversee the mandatory annual privacy training program.

c. Oversee a privacy awareness program.

7.2.2 The NASA Privacy Program Manager shall:

a. Review and approve all privacy awareness and training materials.

b. Develop privacy awareness and training materials.

c. Work with the Information Technology Security Awareness and Training Center (ITSATC) to ensure privacy awareness and training materials meet information security training requirements.

d. Ensure the ensuing training:

(1) For the NASA user explains the policies and procedures for safeguarding PII collected and maintained at NASA.

(2) For the NASA user explains the privacy rules of behavior and consequences.

(3) For the NASA user with access to NASA data, explains that willful disclosure of information to individuals not entitled to Privacy Act records or sensitive privacy information in any form is strictly prohibited.

(4) For persons involved in the design, development, operation, or maintenance of any Privacy Act SOR, or in the maintenance of any record within any SOR, explains the requirements regarding the

protection, use, and release of the Privacy Act records.

(5) For persons involved in the design, development, operation, or maintenance of any PII collection, explains the requirements regarding the protection, use, and release of the records.

e. Determine the annual training requirements for CPMs.

7.2.3 The CPM shall:

a. Participate in privacy role-based training, as required.

b. Ensure awareness and training programs are conducted at the Center level.

7.2.4 The ISO shall:

a. Ensure that all NASA users who have access to the data or who develop or supervise procedures for handling PII are trained and are compliant with policies and procedures for safeguarding PII collected and maintained at NASA.

b. Ensure that persons involved in the design, development, operation, or maintenance of any Privacy Act SOR, or in the maintenance of any record in any SOR, are trained in the requirements regarding the protection, use, and release of the Privacy Act records.

c. Ensure that persons involved in the design, development, operation, or maintenance of any PII collection are trained in the requirements regarding the protection, use, and release of the records.

7.2.5 The NASA user shall:

a. Participate in mandatory privacy training prior to gaining access to NASA information and information systems, and yearly thereafter.

b. Participate in privacy role-based training, as required.

7.2.6 The Center BRT members shall participate in annual BRT training and exercises.

Chapter 8 - Privacy Accountability

8.1 Privacy Accountability Overview

8.1.1 The Privacy Accountability chapter relates to NASA's initiatives to ensure accountability as related to compliance with applicable privacy protection requirements. This chapter includes requirements that ensure NASA's compliance with established privacy controls and includes internal reporting requirements and external reporting requirements.

8.1.2 NASA Privacy Accountability procedures are governed by ITS-HBK-1382.08, Privacy Accountability.

8.2 Privacy Accountability Policy

8.2.1 Internal Reporting Requirements.

a. Internal reporting requirements exist within NASA to internally track compliance with privacy laws, regulations, and NASA's policies and procedures. Internal reporting requirements include metrics, data calls, and status reports. The results of internal reporting requirements are used to create metrics that allow the SAOP and the NASA Privacy Program Manager to evaluate the goals and objectives of the NASA privacy program.

b. NASA Privacy Accountability procedures are governed by ITS-HBK-1382.08, Privacy Accountability.

8.2.1.1 The SAOP shall update NASA senior management on the status of privacy goals and objectives.

8.2.1.2 The NASA Privacy Program Manager shall update the SAOP on relevant privacy metrics.

8.2.1.3 The CPM shall:

a. Update the NASA Privacy Program Manager, Center CIO, and Center CISO on the status of the privacy requirements at the Center.

b. Respond to various privacy related mandates and requests for information from the NASA Privacy Program Manager and NASA Privacy Act Officer.

c. Report any Privacy (PII) or Privacy Act violations, as required by NASA policy and procedures.

d. Track planned, in progress, and completed corrective actions taken to remedy deficiencies identified in compliance reviews.

e. Ensure the NASA Master Privacy Information Inventory (MPII) accurately reflects all electronic and non-electronic collections of information for their respective Center and is up to date at all times.

f. Report all significant privacy related activities (e.g., BRT activities and privacy complaints).

8.2.1.4 The ISO shall:

a. Report to the CPM on the status of compliance with NASA Privacy requirements.

b. Control disclosures from their SOR and maintain accountings of all disclosures of information in accordance with 14 CFR 1212.203.

8.2.1.5 The NASA user shall report any suspected or confirmed unauthorized disclosures of PII in any form to the SOC in accordance with Agency ITS incident reporting procedures.

8.2.2 External Reporting Requirements.

a. NASA has a number of external reporting requirements, including those required by OMB, Department of Homeland Security (DHS), FISMA, OIG, Government Accountability Office (GAO), and Congressional inquiries. For example, NASA is required to report annually to OMB or DHS under FISMA on privacy-related issues, including metrics on PIAs and SORNs.

b. NASA Privacy Accountability procedures are governed ITS-HBK-1382.08, Privacy Accountability.

8.2.2.1 The SAOP shall:

a. Ensure external reporting requirements are met.

b. Respond to external reporting requirements, as appropriate.

c. Approve NASA's privacy reports required by OMB and FISMA.

d. Develop a privacy reviews schedule.

e. Ensure that Privacy Act reviews are conducted, as prescribed by the Privacy Act and OMB A-130 and summarized in ITS-HBK-1382.08, Privacy Accountability.

8.2.2.2 The NASA Privacy Program Manager shall:

a. Produce and provide NASA's privacy reports required by OMB and FISMA to the NASA SAISO and the NASA SAOP.

b. Ensure that privacy reviews are conducted in accordance with the schedule outlined in ITS-HBK-1382.08, Privacy Accountability.

8.2.2.3 The NASA Privacy Act Officer shall coordinate and conduct Privacy Act and OMB A-130 reviews in accordance with the schedule outlined in ITS-HBK-1382.08, Privacy Accountability.

8.2.2.4 The CPM shall:

a. Coordinate FISMA privacy reporting data collection efforts for their Center and report to the NASA Privacy Program Manager, Center CIO, and Center CISO.

b. Coordinate regular Privacy Act reviews in accordance with the Privacy Act and OMB A-130.

Chapter 9 - Privacy Rules of Behavior and Consequences

9.1 Privacy Rules of Behavior and Consequences Overview

9.1.1 The Privacy Rules of Behavior and Consequences chapter summarizes privacy responsibilities outlined within this NPR and identifies consequences for violating the NPR. Consequences are impacted by an individual's level of responsibility and the type of PII involved in the matter.

9.1.2 NASA Privacy Rules of Behavior and Consequences procedures are governed by ITS-HBK-1382.09, Privacy Rules of Behavior and Consequences.

9.2 Privacy Rules of Behavior and Consequences Policy

9.2.1 Privacy Rules of Behavior

Privacy Rules of Behavior include the NASA user responsibilities outlined within the chapters of this NPR and the related handbooks. Specific information on Rules of Behavior is governed by ITS-HBK-1382.09, Privacy Rules of Behavior and Consequences.

9.2.1.1 The SAOP shall:

a. Develop Rules of Behavior for privacy outlined within this NPR and in the associated handbook, as appropriate.

b. Ensure that awareness and training materials include information on privacy Rules of Behavior.

9.2.2 Privacy Consequences

NASA may impose penalties on a NASA user who violates this NPR for privacy related violations. A consequence may range from reprimand to suspension or removal. Specifically, the consequences for violating the privacy-related provisions of this NPR are defined in the Privacy Act, OMB memoranda (e.g., OMB Memorandum M-07-16) and the associated handbook. The consequences available under the Privacy Act range from administrative to criminal sanctions. Specific information on consequences is governed by ITS-HBK-1382.09, Privacy Rules of Behavior and Consequences.

9.2.2.1 The SAOP shall outline the consequences and penalty guidelines related to privacy violations.

9.2.2.2 The NASA Privacy Program Manager shall:

a. Advise the SAOP on appropriate consequences for violating this NPR.

b. Advise the CPM on consequences for violating this NPR at the Center level.

c. Establish requirements and procedures for reporting known, suspected, or likely violations of the privacy requirements of this NPR.

9.2.2.3 The CPM shall provide support to the Privacy Program Manager to ensure adherence to the requirements of this NPR at the Center level.

9.2.2.4 The ISO shall:

a. Meet publication requirements for Privacy Act SOR. Any official who willfully maintains a Privacy Act SOR without meeting the publication requirements is subject to possible criminal penalties or administrative sanctions, or both.

b. Be held accountable for privacy violations of this NPR; penalties range from criminal to administrative.

9.2.2.5 The NASA user shall be held accountable for violations of this NPR and related handbooks. Penalties may include reprimand, suspension, removal, or other appropriate administrative action, fines, additional privacy training or other actions in accordance with applicable laws and Agency disciplinary policy.

9.2.2.6 NASA Users may:

a. Be subject to written reprimand, suspension, removal, or other appropriate administrative action under the following situations:

(1) Knowingly failing to implement and maintain information security controls required by this NPR for the protection of PII regardless of whether or not such action results in the loss of control or unauthorized disclosure of PII.

(2) Failing to report any known or suspected loss of control or unauthorized disclosure of PII.

(3) For managers, failing to adequately instruct, train, or supervise employees in their privacy responsibilities.

b. Be subject to criminal penalties for willful and intentional violations of the Privacy Act.

Appendix A: Definitions

Information in Identifiable Form (IIF). In accordance with section 208(d) of the e-Gov act, IIF is defined as "... any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."

In accordance with OMB Memorandum M-03-22, IIF "... is information in an IT system or online collection: (i) that directly identifies an individual (e.g. name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."

Refer to ITS-HBK-1382.03, Privacy Risk Management and Compliance, for additional information on IIF.

Non-Sensitive Personally Identifiable Information (PII). Non-Sensitive PII is information that is available in public sources the disclosure of which cannot reasonably be expected to result in personal harm.

Member of the Public. Refer to ITS-HBK-1382.03, Privacy Risk Management and Compliance for the distinction of member of the public as it pertains to e-Gov and the PRA.

Personally Identifiable Information (PII). In accordance with M-07-16, PII "... refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

In accordance with M-10-23, "... [t]he definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual."

For purposes of NASA policy, sensitive PII excludes personal information collected and or maintained by NASA employees and contractors for personal rather than NASA business purposes, as allowed under NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology. Examples of such excluded data include contact information for family, relatives, and doctors.

Refer to ITS-HBK-1382.03, Privacy Risk Management and Compliance, for additional information on PII.

Privacy Impact Assessment (PIA). In accordance with M-03-22, a PIA "... is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate

potential privacy risks."

Refer to ITS-HBK-1382.03, Privacy Risk Management and Compliance for additional information on PIAs.

Privacy Breach. A privacy breach is also known as an "incident." An incident is any adverse event or situation associated with any information collection containing PII that poses a threat to integrity, availability, or confidentiality. An incident may result in or stem from any one of the following: a failure of security controls; an attempted or actual compromise of information; and/or waste, fraud, abuse, loss, or damage of government property or information. Refer to ITS-HBK-1382.05, Privacy Incident Response and Management, for specific information on privacy breach.

Sensitive Personally Identifiable Information. This definition is related to incident reporting only as outlined in Chapter 5 of this NPR. All PII, regardless of whether it is sensitive or non-sensitive, shall be protected as outlined in this NPR and as defined in OMB Memorandum M-07-16.

Sensitive PII is a combination of PII elements, which if lost, compromised, or disclosed without authorization could be used to inflict substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Refer to ITS-HBK-1382.05, Privacy Incident Response and Management, for the distinction of sensitive versus non-sensitive PII.

Appendix B: Acronyms

BRT	Breach Response Team
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer (Formerly known as ITSM)
CO	Contracting Officer
COPPA	Children's Online Privacy Protection Act
COTR	Contracting Officer's Technical Representative
CPM	Center Privacy Manager
DHS	Department of Homeland Security
e.g.	Exempli gratia (for example)
e-Gov Act	E-Government Act of 2002
FAR	Federal Acquisition Regulations
FAQ	Frequently Asked Question
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GAO	Government Accountability Office
GOCO	Government Owned, Contractor Operated
HBK	Handbook
ICAM	Identity, Credential, and Access Management
i.e.	id est (that is)
IIF	Information in Identifiable Form
IP	Internet Protocol
IPTA	Initial Privacy Threshold Analysis
ISO	Information System Owner
ITS	Information Technology Security
ITSATC	Information Technology Security Awareness and Training Center
JPL	Jet Propulsion Laboratory (an FFRDC)
MPII	Master Privacy Information Inventory
NASA	National Aeronautics and Space Administration

NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
P.L.	Public Law
PPM	Privacy Program Manager
PRA	Paperwork Reduction Act
SAISO	Senior Agency Information Security Officer
SAOP	Senior Agency Official for Privacy
SOC	Security Operations Center
SOR	System of Records
SORN	System of Records Notice
SP	Special Publication
SSN	Social Security Number
U.S.C.	United States Code

Appendix C: Responsibility Cross-Walk

	NASA Administrator	NASA CIO	SAOP	NASA Center Director	Center CIO	SAISO	NASA PPM	NASA Privacy Act Officer	Center CISO	CPM	ISO	System Manager
2 - Overarching (Chapter 2)	2.1.2.1	2.1.2.2	2.1.2.3	2.1.2.4	2.1.2.5	2.1.2.6	2.1.2.7	2.1.2.8	2.1.2.9	2.1.2.10	2.1.2.11	
3 - Privacy Risk Management and Compliance (See HBK 1382.03)			3.2.1.1 3.2.2.1 3.2.3.1 3.2.4.1 3.2.5.1		3.2.2.2		3.2.1.2 3.2.2.3	3.2.3.2 3.2.4.2 3.2.5.2		3.2.1.3 3.2.2.4 3.2.3.3 3.2.4.3	3.2.1.4 3.2.2.5 3.2.3.4 3.2.4.4 3.2.5.3	
4 - Privacy and Information Security (See HBK 1382.04)			4.2.1						4.2.2	4.2.3	4.2.4	
5 - Privacy Incident Response (See HBK 1382.05)			5.2.1		5.2.2		5.2.3			5.2.4	5.2.5	
6 - Privacy Notice and Redress (See HBK 1382.06)		6.2.1.1	6.2.1.2 6.2.2.1 6.2.4.1 6.2.5.1		6.2.1.3 6.2.2.2		6.2.1.4 6.2.2.3 6.2.3.1 6.2.4.2 6.2.5.2	6.2.5.3		6.2.1.5 6.2.2.4 6.2.4.3 6.2.5.4	6.2.1.6 6.2.2.5 6.2.3.2 6.2.4.4	6.2.5.5
7 - Privacy Training and Awareness (See HBK 1382.07)			7.2.1				7.2.2			7.2.3	7.2.4	
8 - Privacy Accountability (See HBK 1382.08)			8.2.1.1 8.2.2.1				8.2.1.2 8.2.2.2	8.2.2.3		8.2.1.3 8.2.2.4	8.2.1.4	
9 - Privacy Rules of Behavior and Consequences (See HBK 1382.09)			9.2.1.1 9.2.2.1				9.2.2.2			9.2.2.3	9.2.2.4	

	NASA User	OIG	Office of General Counsel	Center Chief Counsel	Center Public Affairs Office	CO/COTR	Center Human Resources Employee Relations	FOIA Officer
2 - Overarching (Chapter 2)	2.1.2.12							
3 - Privacy Risk Management and Compliance (See HBK 1382.03)								
4 - Privacy and Information Security (See HBK 1382.04)	4.2.5							
5 - Privacy Incident Response (See HBK 1382.05)	5.2.6	5.2.7	5.2.8	5.2.9	5.2.10	5.2.11	5.2.12	

6 - Privacy Notice and Redress (See HBK 1382.06)								6.2.5.6
7 - Privacy Training and Awareness (See HBK 1382.07)	7.2.5							
8 - Privacy Accountability (See HBK 1382.08)	8.2.1.5							
9 - Privacy Rules of Behavior and Consequences See HBK 1382.09)	9.2.2.5 9.2.2.6							

Appendix D: Role Definitions

	Role	Definition
D.1	NASA Chief Information Officer (CIO)	The principal advisor to the Administrator and other senior officials on matters pertaining to information technology.
D.2	Senior Agency Official for Privacy (SAOP)	The principal advisor to the NASA Administrator and other senior officials on matters pertaining to privacy.
D.3	Center Chief Information Officer (CIO)	The principal advisor to the NASA CIO and senior Center officials on matters pertaining to information technology.
D.4	Senior Agency Information Security Officer (SAISO)	The principal advisor to the NASA CIO and other senior officials on matters pertaining to information security.
D.5	NASA Privacy Program Manager	The principal advisor to the SAOP on matters pertaining to privacy. Responsible for the day-to-day operations of the NASA Privacy program.
D.6	NASA Privacy Act Officer	The principal advisor to the NASA Privacy Program Manager on Privacy Act Matters. Responsible for NASAs Privacy Act compliance activities.
D.7	Center Chief Information Security Officer (CISO)	The principal advisor to the SAISO, Center CIO, and senior Center officials on matters pertaining to information security.
D.8	Center Privacy Manager (CPM)	The principal advisor to the Center Director, Center CIO, Center CISO, and ISOs on matters pertaining to privacy and acts as Privacy Act liaison with the NASA Privacy Act Officer. Responsible for the day-to-day operations of the Center Privacy program.
D.9	Information System Owner (ISO)	The principal advisor to the Center CISO on matters pertaining to specific information systems. As it pertains to this NPR, ISO responsibilities apply to an Information Owner of a collection of PII, as appropriate.
D.10	System Manager	The NASA official who is responsible for a SOR, as designated in the system notice of that SOR published in the Federal Register. When a SOR includes portions located at more than one NASA Center, the term system manager includes any subsystem manager designated in the system notice as being responsible for that portion of the SOR located at the respective Center.
D.11	NASA User	Any explicitly authorized patron of a NASA information system. The NASA user includes, but is not limited to, civil servants and contractors.

Appendix E: References

E.1 OMB Memorandum M-1-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy.

E.2 OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

E.3 OMB Memorandum M-10-06, Open Government Initiative.

E.4 Best Practices: Elements of a Federal Privacy Program, version1.0, June 2010, Federal CIO Council Privacy Committee.